When Reputation is Not Enough: Barracuda Spam & Virus Firewall Predictive Sender Profiling

RELEASE 1
APRIL 2007

As spam continues to evolve, Barracuda Networks remains committed to providing the highest level of protection against the latest spam trends. When image spam first began its assault on email users in early 2006, Barracuda Networks was one of the first anti-spam vendors to provide Optical Character Recognition (OCR) capabilities to defend against this threat. Throughout the growth of image spam volume, Barracuda Spam & Virus Firewall's OCR techniques enabled it to maintain its target 95 percent effectiveness rating in the fight against spam with almost no false positives. Today, while the volume of image spam has remained stable, spammers have significantly increased the usage of yet another technique – sender identity obfuscation.

Barracuda Central: 24x7 Operation

Barracuda Networks stays ahead of spammers through Barracuda Central, an advanced technology center consisting of highly trained engineers that monitor the Internet for the latest trends in spam and virus attacks, and develop strategies to mitigate those threats. As new forms of spam and viruses emerge, Barracuda Central is quick to respond to early outbreaks and delivers the latest definitions through Barracuda Energize Updates delivered every 30 minutes. Barracuda Central operates 24-hours-a-day, seven-days-a-week and has access to a diverse network of spam traps ("honeypots"), as well as more than 70,000 Barracuda Spam & Virus Firewalls worldwide, amassing the most diverse compilation of active email traffic representing Internet Service Providers, government institutions, enterprises, and small and medium businesses. Using this expansive corpus of email, Barracuda Central is able to detect the latest spam trends and can develop tactics to alleviate those threats in real-time.

Reputation vs. Profiling Techniques

Traditionally, reputation techniques have been used to combat spammers by profiling the sender's history. Barracuda Networks utilizes a two-fold approach in determining an email sender's reputation: Barracuda Reputation Analysis and Intent Analysis. Both Reputation and Intent Analysis, like many traditional reputation techniques, enable the Barracuda Spam & Virus Firewall to block spam efficiently by doing a simple database lookup.

However, as spammers become more organized and more creative in their tactics, they have resorted to obfuscating their identities more systematically, rendering reputation data less effective on its own. Blocking these new forms of spam email requires the use of techniques that can profile the behavior of the sender and identify any uncharacteristic activity. Profiling techniques, such as Barracuda Networks Predictive Sender Profiling, are designed to look beyond the apparent reputation of the sender and dig deeper into the campaign itself to identify anomalous activity.

Introducing Predictive Sender Profiling

Consider this example: In the credit card industry, consumers' reputations are profiled through credit scores, which essentially reflect the consumers' purchasing history. If consumers are consistent in their buying habits, their reputations are easy to follow and their future buying activities are likely predictable. However, what if a consumer with historically consistent buying habits purchases a television at a popular retail store and then shortly after leaving the store, returns and purchases the same television within 30 minutes of the original purchase? Better yet, what if the consumer purchases 15 more televisions within the first 30 minutes of the original purchase? The credit card company would flag this as anomalous behavior and would likely contact the consumer to verify the subsequent purchases to make sure that the consumer's credit card has not been stolen. Predictive Sender Profiling behaves in a similar fashion to the credit card company in this example.

When legitimate email senders abide by the rules of sending email, they build trusted reputations and their email behavior becomes easy to predict. If a typically good, or reputable, email sender sent a slew of email all at once, reputation databases would not flag the sender as a potential spammer because their past behavior was so pristine. Predictive Sender Profiling, however, profiles behavior independent of the sender's past activity and would detect this uncharacteristic behavior and act accordingly by blocking unwanted email.

Barracuda Intent Analysis

All spam messages have an "intent" – which is to get a user to reply to an email, visit a Web site or call a phone number. Intent analysis involves researching email addresses, Web links and phone numbers embedded in email messages to determine whether they are associated with the legitimate entities. Frequently, intent analysis is the defense layer that catches phishing attacks.

Barracuda Reputation Analysis

Barracuda Reputation Analysis is maintained by Barracuda Central and tracks the history of IP addresses on the Internet. From Barracuda Reputation data, two lists are maintained for use by the Barracuda Spam & Virus Firewall - a list of identified spammers (a "blacklist") and a list of recognized good senders (a "whitelist"). Updates to the Barracuda Reputation database are delivered to the Barracuda Spam & Virus Firewall via the Barracuda Energize Updates service.

Reputation Alone Falls Short Against Botnets & Zombies

Sender identity obfuscation techniques often involve spammers taking control of networks of computers infected with malware (also called "botnets"), and sending email from diverse sources throughout the Internet. In doing so, the spammer effectively hides their own identity from traditional reputation checks that profile sender network addresses.

For example, in illustrations A, B, and C below, the spammer attempts to hide their identity by sending out virtually the same message from different addresses around the world. In illustration A, the message is detected as originating from an IP address in Germany. One day later, in illustration B the same message is picked up as coming from the UK and by the third day of the campaign, Barracuda Central had identified the message again, this time coming from Spain. Clearly, in this example, the spammer had overtaken a series of computers (botnets) and used them for this particular campaign pushing Viagra and Cialis.

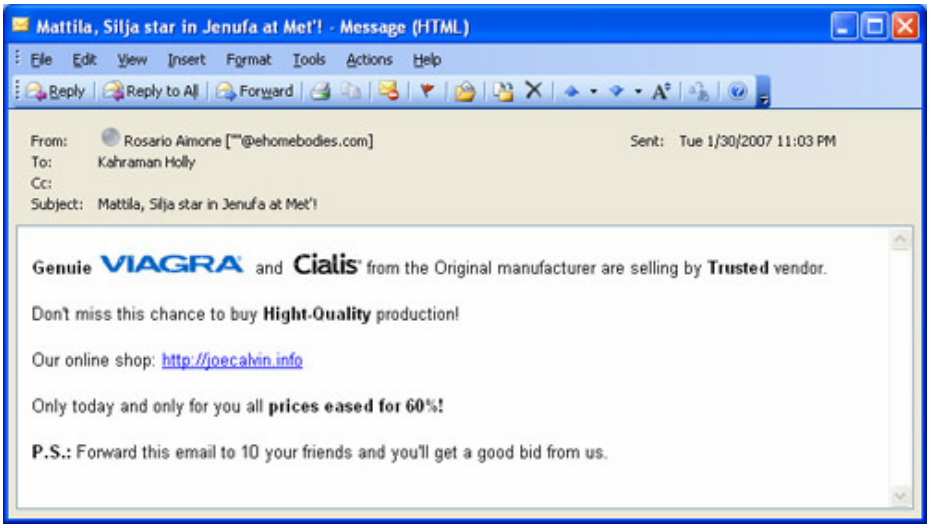

Illustration A: *IP Address 84.163.90.168 (Deutsche Telekom, Germany)*

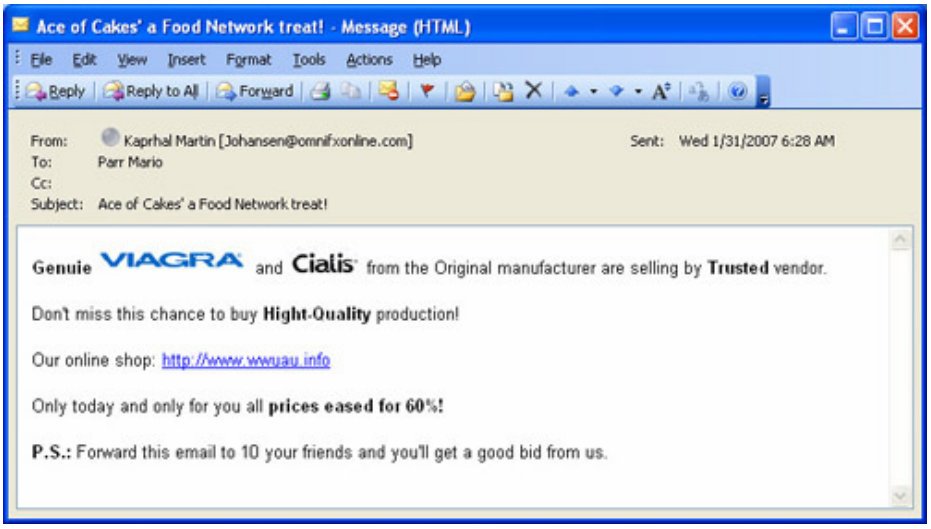

Illustration B: *IP Address 84.13.58.219 (Opal Telecom, United Kingdom)*

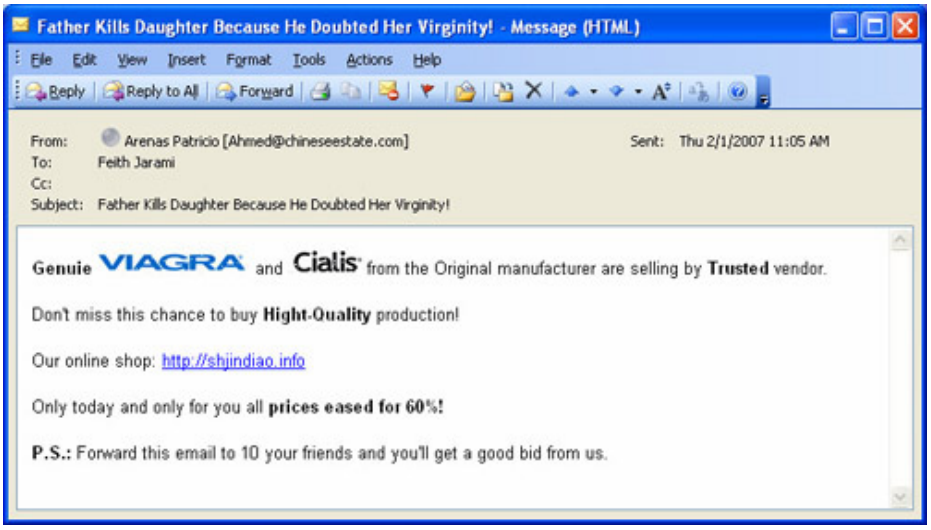

Illustration C: *IP Address 217.125.88.118 (Telefonica-Data-España, Spain)*

In addition to sending from different IP addresses, these sample emails all used different embedded URLs in an attempt to bypass Intent Analysis. In Illustration A, the URL points to *http://joecalvin.info*, in Illustration B, the URL points to *http://www.uau.info*, and in Illustration C, the URL points to *http://shjindaio.info*. Just as botnets have enabled spammers to send from many sender IP addresses, cheap domain registrations have enabled spammers to create new domain identities quickly and inexpensively.

Despite the inability to utilize traditional reputation techniques on these emails, the Barracuda Spam & Virus Firewall, blocked these messages by profiling the sender's behavior and predicting new instances of this email. In this case, the profiled behavior was derived from the need to provide domain name services (DNS) for all of the new domains. By recognizing that the spammer configured all of the new domains with the similar DNS settings as their known spam domains, the Barracuda Spam & Virus Firewall was able to block all instances of these emails using its Real-time Intent Analysis capabilities.

Hiding Behind the "Good Guy"

By registering new domains or by redirecting to spam Web domains through reputable blogs, free Web site providers, or URL redirection services, spammers have also learned to hide their identity from traditional reputation checks that profile spam Web domains.

Illustrations D and E below show two separate spamming campaigns that were recently detected by Barracuda Central in which the spammers attempt to hide their identity by using URLs referencing reputable Web domains, Geocities and Blogspot. Often these URLs contain either redirections or simple Web links to known spammer Web sites.

Despite these attempts to hide behind a "good" identity, the Barracuda Spam & Virus Firewall profiled this campaign behavior of placing redirections or Web links to known spam sites behind popular Web providers. The Barracuda Spam & Virus Firewall was able to block these messages through Multi-level Intent Analysis by following the embedded URLs as a Web browser would and inspecting the resulting contents.

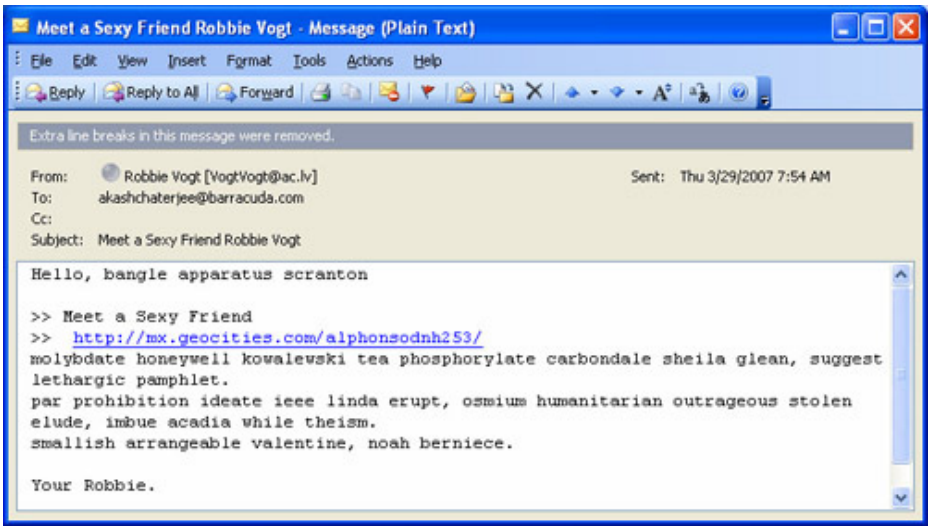

Illustration D: *Geocities redirect to sexdatasearch.com - known spammer*

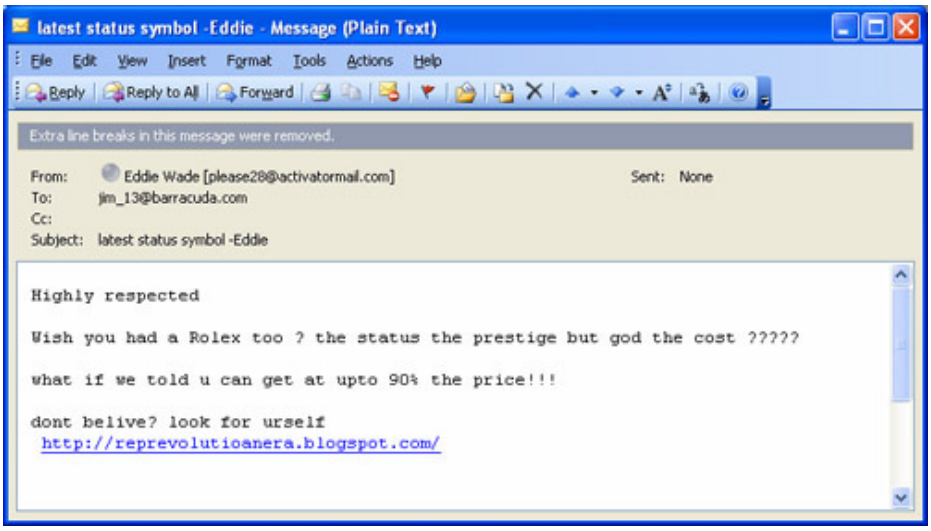

Illustration E: *Blogspot redirect to known spammer IP (211.93.46.38)*

Sample Behaviors & Countermeasures

When spammers obfuscate their identities, the Barracuda Spam & Virus Firewall can use Predictive Sender Profiling to identify behaviors of all senders and apply the applicable Barracuda Spam & Virus Firewall defense tactic. Examples include:

Behavior: **Sending too many emails from a single network address**
Automated spam software can be used to send large amounts of email from a single email server.

Countermeasure: Rate Control
To protect the email infrastructure from these flood-based attacks, the Barracuda Spam & Virus Firewall counts the number of incoming connections from a particular IP address and throttles the connections once a particular threshold is exceeded.

Behavior: **Attempting to send to too many invalid recipients**
Many spammers attack email infrastructures by harvesting email addresses.

Countermeasure: Recipient Verification
The Barracuda Spam & Virus Firewall automatically rejects SMTP connection attempts from email senders that attempt to send to too many invalid recipients, a behavior indicative of directory harvest or dictionary attacks.

Behavior: **Registering new domains for spam campaigns**
Because registering new domain names is fast and inexpensive, many spammers switch domain names used in a campaign.

Countermeasure: **Real-time Intent Analysis**
Used for new domain names that may come into use, real-time intent analysis involves performing DNS lookups and comparing DNS configuration of new domains against the DNS configurations of known spammer domains.

Behavior: **Using free Internet services to redirect to known spam domains**
Use of free Web sites to redirect to known spammer Web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as intent analysis.

Countermeasure: **Multilevel Intent Analysis**
Multilevel intent analysis involves inspecting the results of Web queries to URLs of well-known free Web sites for redirections to known spammer sites.

Summary

Barracuda Central is well positioned to keep spam under control. Leveraging the industry's most expansive corpus of email from over 70,000 customer systems ranging from small and medium businesses to Internet Service Providers and large enterprises, Barracuda Central is well positioned to stay abreast of the latest Internet threats.

For computationally efficient processing of email, Barracuda Networks leverages this email corpus to provide industry-leading reputation data for both IP addresses through Reputation Analysis and Internet domain names through Intent Analysis.

Moving forward, as the usage of sender identity obfuscation increases, Predictive Sender Profiling makes the Barracuda Spam & Virus Firewall well equipped to protect against spam that is typically unstoppable by traditional reputation filters

For questions about the Barracuda Spam & Virus Firewall, please visit http://www.barracuda.com/spam or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com